



BENCHMARKS

The University of North Texas Computing Center Newsletter

VOLUME 12 NUMBER 3
March 1991

A UNIX* System for Research

By Billy Barron, VAX/UNIX System Manager (BITNET: BILLY@UNTVAX)

Academic Computing Services has recently purchased a Solbourne SE/902 UNIX computer system for central campus use. The hardware was installed on February 13th and, hopefully, the system will be fully in production by the end of March.

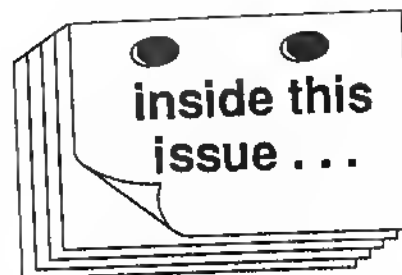
The Solbourne SE/902 is a Sun-compatible UNIX server system. It runs Solbourne OS/MP which is a slightly modified version of SunOS. The Solbourne will run all Sun applications and can use most of the Sun hardware peripherals, but is more expandable than the Sun systems and has better price/performance.

The Solbourne SE/902 is a two processor system, though it can be expanded up to eight processors. The two processor system we have purchased is capable of 60 MIPS (Millions of Instructions Per Second), 8 double-precision MFLOPS (Megaflops), and 36 SPECthroughs. The Solbourne has 64 MB of main memory and 1.7 GB (gigabytes) of disk storage. Plans are to add processors and disks if more are needed to meet demand.

The Solbourne's major purpose will be to provide the research community with sufficient horsepower to handle their CPU intensive tasks. If spare capacity exists, then the Solbourne will also be used for instructional use.

* UNIX is a registered trademark of AT&T Bell Laboratories.

Continued on page 3.



□ UNIX

A UNIX System for Research	1
UNIX Systems Programmer Hired	3
Solbourne and UNIX	3
D/FW UNIX User's Group	8
The UNIX Shell	9

□ GENERAL INFORMATION

On-line Bibliographic Data Base Document Updated	10
Internet-Accessible BBSs	11
Mailing Binary Files	11
The BITNET Connection	12
LIST of the Month	13
Staff Activities	14
BENCHMARKS FORUM	15
OS/MVS JCL Utilities: IEBCOMPR	17
Spring Break Lab Hours	18

□ MICROCOMPUTERS

Some PC Viruses Described	19
MICRO-TIPS	19
DrawPerfect Demo Scheduled	20

□ VAX COMPUTER CLUSTER

Best of the BBS	28
Disk Backup Schedules	28





SERVICES AVAILABLE TO USERS OF THE UNT COMPUTING FACILITIES

The UNT Computing Center is located in the Information Sciences Building (ISB), Room 119. Phone Numbers:

Computing Center: (817) 565-2324
Help Desk: (817) 565-4050
Micro Support: (817) 565-2316, 565-2319
Graphics Lab: (817) 565-3479
ISB I/O Area: (817) 565-3890
BA I/O Area: (817) 565-2350

All personnel listed below can be contacted either by calling the Computing Center or by sending them electronic mail on VM/CMS (ID-codes follow each name. All IDs are on BIT-NET node UNTVM1).

Benchmarks - Claudia Lynch (AS04)

Information & ID-Codes; Disk Space Problems, Passwords - Theresa Ruesell

Statistical/Research Support - George Morrow (AS01), Panu Sittiwong (AC08), Phanit Laosirirat (AC44)

Academic ADABAS/COM-LETE - Cathy Hardy (AC55)

CRSP & COMPUSTAT Problems - Panu Sittiwong (Panu), Phanit Laosirirat (AC44)

Student Programming Problems - CSCI Dept., GAB Room 550; BCIS Dept., BA Room 152

Problems with JCL, Operating Systems, or Communication/Terminal Problems - Help Desk

Data Entry; Test Scoring & Analysis - Betty Grise

Administrative Applications - Coy Hoggard

Printout Retrieval - ISB or BA I/O Operators



DIALING-UP UNT COMPUTERS OVER THE TELEPHONE

Phone numbers for accessing UNT computing systems:

300-2400 BAUD: (817) 565-3300
 300/1200 BAUD: (817) 565-3499
 300-9600 BAUD: (817) 565-3461
 300-2400 BAUD: D/FW METRO 792-4140

Area code 214 must dial 817 before the METRO #.

In your communications program, set Data Bits to 7, Parity to S, and Stop Bits to 1. The dial-up numbers have an autobaud feature that requires you to hit the <RETURN> key repeatedly once a connection with the remote modem is made. This is so that the receiving modem can determine the appropriate baud rate. When you have established a communications link, a prompt (# for non-metro numbers, UNTModem# for the metro lines) will appear on your screen and you can enter one of following commands to connect with the system of your choice.

Metro Lines UNTModem#	Non-Metro Lines #	System
N/A	CALL 8040	MUSIC/SP (line editing and PCWS)
Connect VM3270	CALL 3270	Academic Mainframe Full Screen (MUSIC, CMS, Academic COM-LETE)
Connect DEC	CALL DEC	VAXcluster (VMS)
Connect Sol	CALL 900	Solbourne (Unix)
Connect Ponder	CALL 780	Sequent (Ponder)
Connect Library	CALL 3000	UNT Libraries on-line card catalogue.

HOURS FOR UNIVERSITY OF NORTH TEXAS COMPUTER ACCESS AREAS : Spring 1991*

Location	Days	Times
Computing Center RJE	Sunday Monday-Saturday	Noon-Midnight 7 a.m. Mon.-Midnight Sat. (Open 24 hours/day)
ISB 110 Terminal Area	Sunday Monday-Thursday Friday Saturday	1-11:50 p.m. 8:00 a.m.-11:50 8:00 a.m.-8:50 p.m. 9 a.m.-8:50 p.m.
College of Business	Sunday Monday-Thursday Friday, Saturday	Noon-Midnight 8:15 a.m.-11:45 p.m. 8:15 a.m.-7:45 p.m.
GAB 550	Sunday Monday-Thursday Friday Saturday	2 p.m.-Midnight 8 a.m.-Midnight 8 a.m.-3 p.m. CLOSED
Graphics Lab	Sunday Monday-Thursday Friday Saturday	1 p.m.-Midnight 8 a.m.-Midnight 8 a.m.-9 p.m. 9 a.m.-9 p.m.
Willis Library	Sunday Monday-Thursday Friday Saturday	1 p.m.-Midnight 7:30 a.m.-Midnight 7:30 a.m.-9 p.m. 9 a.m.-9 p.m.

*Hours may vary. Check MUSIC/SP, VM/CMS, VAX, or Solbourne NEWS and/or posted schedules for exceptions.

This issue of Benchmarks was produced by the Documentation Services section of Academic Computing using Xerox Ventura Publisher on a 386SX clone and printed on an Apple LaserWriter IINT. Unless otherwise noted, articles or information may be reproduced for nonprofit purposes provided the publication and issue are fully acknowledged.

It is hoped that some VAX and Mainframe users will off-load their applications from these platforms to the Solbourne. The Solbourne system has the best price/performance ratio of any central computing resource on campus so it is in the University's best interest to utilize this resource (whenever possible) instead of the VAX and the Academic HDS Mainframe.

C, FORTRAN 77, DISSPLA, X-windows, and SAS are some of the software packages that will be initially supported on the Solbourne. More software will be added at a later time.

The usage policies for the Solbourne, as approved by the Information Resources Council (formerly known as the Computing Council) are:

Individual Accounts

- ① All faculty and academic support staff will be given individual accounts on the system if they request them, provided they get the approval of their departmental account authority.
- ② All graduate students will be given individual accounts on the system, provided they get the approval of their departmental account authority.
- ③ No undergraduate students will be allowed to have individual accounts during the Spring, 1991 semester. This policy will be reevaluated prior to the beginning of the Fall, 1991 semester.

Instructional Use

- ① Since the system is not likely to be delivered, installed, and configured prior to March, 1991, it will be impossible to accommodate instructional needs during the Spring, 1991 semester.
- ② We will allow a limited number of instructional class accounts during the Summer, 1991 session.
- ③ Provided adequate capacity is available, we will allow instructional class accounts beginning with the Fall, 1991 semester.
- ④ If capacity proves insufficient to meet research needs and no additional funding is available for expansion of the system, we will allow instructional accounts only in those cases where the use of the Unix system or applications running on that system is essential to pedagogical goals, and that these goals cannot be met through the use of other systems.

In conclusion, the Solbourne system will provide UNT with some much needed computing horsepower especially for the research community. It should be a good step helping UNT "emerge" as a research institution. ■

St.-Gil Hired as UNIX Systems Programmer

Marc St.-Gil, a 1988 graduate of UNT with a B.S. degree in Computer Science, has been hired as the UNIX Systems Programmer for the Solbourne. Prior to his current employment here at UNT, Marc worked as a software engineer for Harris Adacom Corp. in the Research and Development department. Marc's expertise adds a new dimension to Academic Computing. We are pleased to have him on our staff. His office is located in the "Academic Computing hall," accessible through ISB 119. ■

Solbourne and UNIX: an Introduction

By Billy Barron, VAX/UNIX System Manager (BITNET: BILLY@UNT.VAX)

The Solbourne 5E/902 is a multi-processing Sun compatible Unix machine. All Sun SPARC software will run on the Solbourne without modification. The 5E/902 system is a 60 MIPS, 8 MFLOPS machine. The Solbourne will be initially a research oriented machine. If sufficient processing power is available, then undergraduate students will be allowed access in Fall 1991.

The UNIX operating system was originally developed by AT&T Bell Labs and has primarily been used as a research-oriented operating system. At the current time, it is penetrating the commercial market place.

UNIX is not an easy operating system to learn, but it is very powerful. However, with some effort anyone can learn the Unix operating system.

Access through the Sytek Local Area Network (LAN)

If you are attempting to access the Solbourne via the Sytek LAN (# prompt) from a terminal, you will need to do so by placing a call over the campus-wide Local Area Network. This can be accomplished by entering the following:

ECHO OFF

or, if calling the 3300 Dialup Line:

ECHO REMOTE

[Turns off local character echoing]

CALL 900

[To access Solbourne]

If all of the available ports are busy, the following message will appear on your terminal:

To access the Solbourne via the Sytek Local Area Network, at the # prompt, type :

**# ECHO OFF
CALL 900
or, if calling the 3300 Dialup Line
#ECHO REMOTE
Connect Sol**

UNABLE TO OPEN SESSION -
REMOTE PORT (S) BUSY

Wait a few minutes and try again. If you receive the message,

UNABLE TO OPEN SESSION - NO
RESPONSE FROM UNIT

one of the host ports is probably out of service and being repaired. If you receive this message, try calling one of the other ports on the Solbourne. The ports for the Cluster range from 900 to 906 in hexadecimal (2 ports per address). A successful call over the Sytek LAN will result in the following response:

CALL COMPLETED TO 900.0
[or the address that you called]

Press the <RETURN> key a few times and the UNIX login procedure will prompt you for a Userid (the login: prompt) and a Password. Once you have entered the appropriate information, you will be logged onto the system. Note: your userid must be typed in lowercase.

Accessing via the New Metro Dialup Lines

If you are calling the 817-792-4140 Metro dialup lines, type Connect Sol at the UNT MODEM> prompt. You can then follow the same UNIX login procedure described above.

Accessing via the Internet

Telnet to the address SOL.ACS.UNT.EDU. On most systems, it is just the command: **TELNET SOL.ACS.UNT.EDU**. Consult the documentation on your TCP/IP package for more details.

Entering Commands

Once you have successfully logged

To access the Solbourne via the Internet type:

TELNET SOL.ACS.UNT.EDU

onto the Solbourne, you will see the C-Shell prompt (%). Commands are entered by typing a series of characters and pressing <RETURN>. Almost all UNIX commands are lowercase. UNIX is case-sensitive and therefore uppercase commands do not work.

Commands are typically very terse (often a word with the vowels missing). Commands can be modified by flags. Flags follow commands on the command line with a space, a - (hyphen), and then the flag (or flags).

Important Keys

<CTRL>-S
[Suspends screen output]

<CTRL>-Q
[Resumes screen output]

BS or Backspace
[Delete character to the left of the cursor]

<CTRL>-C
[Terminate program]

<CTRL>-Z
[Suspend program]

<CTRL>-X
[Erase to beginning of line]

Changing Your Password

If you are logging on for the first time, you should change your password to something unique that you will remember. We also recommend that you change your password on a fairly regular basis as a security precaution. Due to the way UNIX passwords are stored, it is HIGHLY recommended that you do not use any word in the dictionary. In order to change your

password, at the dollar sign prompt type:

\$ passwd

The new password goes into effect upon your next login.

The man Command

The **man** command invokes the UNIX manual facility to display information about a UNIX command or topic. Type **man** at the % prompt and the system will display a list of commands and prompt for a topic.

If you are not sure of the command, you can use the **man -k <subject>** command. It will list the heading of all

The man command invokes the UNIX manual facility to display information about a VMS command or topic. Type man at the % prompt and the system will display a list of commands and prompt for a topic.

manual listings that related to the subject. For example:

```
% man -k directory
cd (1) — change working directory
chdir (2) — change current working directory
chdir (3F) — change working directory
chroot (2) — change root directory
ls (1) — list contents of directory
mkdir (1) — make a directory
mkdir (2) — make a directory file
pwd (1) — working directory name
```

The number in parantheses is the manual section. The UNIX manuals is divided into 8 sections:

- ① Commands
- ② System Calls
- ③ Subroutine Library
- ④ File Formats
- ⑤ Miscellaneous Facilities
- ⑥ Games
- ⑦ Devices
- ⑧ Administration Commands.

In many cases, the same topic will be in multiple sections (e.g. mkdir in the above example). By default, the man command displays the first section it finds the topic in. To over-ride this, you can type man # <topic> for a particular section, where # stands for a number. For example:

```
% man 2 mkdir
```

Unix Manuals

Manuals are available on practically every aspect of the Unix operating system. A complete set of manuals needed for use can be found in the ISB 110 lab.

Logging Out

To end a Solbourne session, type :

```
% CTRL-D
```

Filenames

Filenames can have from one to 255 characters chosen from any character except "*", "?", or "/". Additionally, filenames cannot start with a "-". Any file with a filename starting with "." is known as a hidden file. Normally, hidden files do not show up in directory listings, etc without the use of special options.

Wildcards

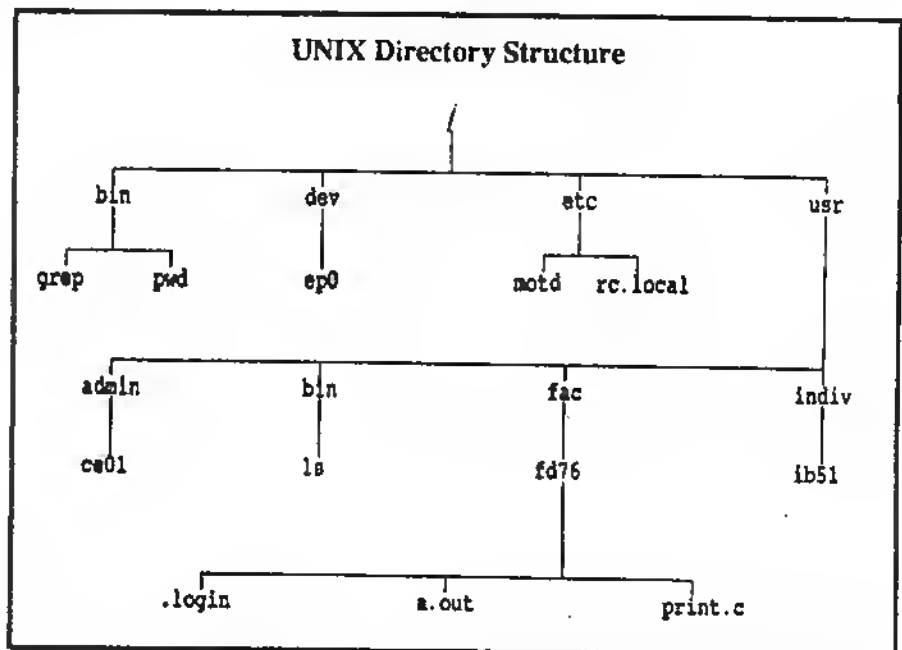
A wildcard character can be used with all UNIX commands to execute the command on several files at once instead of each file individually. The two wildcard characters are ? and *.

The ? wildcard character replaces a single character in the filename. For example, the filename *letter?.txt* count mean the files *letter1.txt*, *letter2.txt*, and *letters.txt*. However, *letters1.txt* would not apply because the ? would need to replace two characters.

The * wildcard character replaces any number of characters in the filename. For example, the filename *letter*.txt* includes the files *letter1.txt*, *letter2.txt*, *letters.txt*, and *letters1.txt*.

Directories

A directory is a collection of files that are stored together. Usually, the files are stored together because they are somehow related to each other. UNIX has a hierarchical directory structure where a directory can contain other directories. An example directory structure is shown below.



The / directory is also known as the root directory. The / character is also used to delimit between different directories.

Examples (based on the directory structure to the right):

```
/
/bin
/etc
/usr
/usr/admin
/usr/fac
/usr/fac/fd76
```

To access files in other directories, just add a / character and the filename to end of the above directory specifications.

Examples (based on the directory structure above and to the right):

```
/bin/grep
/usr/bin/ls
/usr/fac/fd76/a.out
```

When using UNIX, the you have acurrent directory. This allows many directory specifications to be shortened. If the directory specification does not start with a /, the current directory specification is prepended to the directory specified. For example, if the current directory is /usr, then to access the /usr/fac directory, only fac needs to be specified.

Likewise, to access the file ls in the /usr/bin directory, only bin/ls needs to be specified.

Another directory specification is ".." (period period). ".." is the directory immediately above the current directory in the heirarchy. For example, if the current directory was /usr/indiv, the .. directory would be /usr.

Commands to Manipulate Files

The ls command is used to list files in a directory.

```
% ls
Mail      dead.letter  mbox  tmp      x.setup
Makefile  down.c      network2.txt  vi.ref  xstart
```

The -a (all) flag also lists the hidden files. Finally, the -l (long) flag adds protection information, file ownership, file size, and modification date to the listing.

```
% ls -l
drwx---  2 ac02      24 Nov 9   14:48 Mail
-rw-r---  1 ac02    3163 Jul 10   15:52 Makefile
-rw---   1 ac02      9 Sep 11   11:42 dead.letter
-rw-r---  1 ac02   8310 Jul 11   14:37 down.c
-rw---   1 ac02   1882 Sep 20   16:20 mbox
-rw-r-r-  1 ac02   73197 Aug 30   15:52 network2.txt
drwxrwx-- 2 ac02     512 Dec 11   09:43 tmp
-rw-rw-rw- 1 ac02  16701 Dec 19   11:52 vi.ref
-rwxr---  1 ac02    440 Dec 14   15:34 x.setup
-rwxr-x-- 1 ac02    925 Dec 14   15:34 xstart
```

The first character will be either a "d" or a "-". A "d" means directory. A "-" means a regular file. The next nine characters are protections (see the file protection section below). The number following that is the number of links the file has. Under normal circumstances, this number can be ignored. The next field is the owner of the file. Following that is the file size in bytes, the date the file was last modified, and the filename itself.

- The more Command will display a file at your terminal.

```
% more vi.ref
```

- To get a hardcopy printout of a file you can log onto a hardcopy terminal and use the TYPE command or type PRT from any other terminal. If you use the PRT utility, you will be given several options for printing your file.
- The cp command makes copies of files. You specify first the name of the input file you want to copy, then the name of the output file. The following cp Command copies the contents of the file payroll.lst to a file named payroll.old.

```
% cp payroll.lst payroll.old
```

- The mv Command changes the name of one or more files. This example changes the name of the file payroll.dat to test.old

```
% mv payroll.dat test.old
```

- The **rm** Command deletes specific files.

% **rm a.out**

- You can create subdirectories in any directory in which you can create files. This ability can help keep files organized since you can place categories of files in the same subdirectory.

% **mkdir bin**

- To access files in this subdirectory, use the **cd** Command.

% **cd bin**

To move to the next highest level directory, type:

% **cd ..**

The **cd** Command with no parameters will return you to your main directory.

- Directories can be deleted with the **rmdir** command. The directory to be removed needs to have all the files within it deleted first.

% **rmdir bin**

File Protections

UNIX breaks file protection into three classifications:

user	the owner of the file
group	any user in the same group as the owner
other	any other user

Each of these classifications has three possible modes of access to the file:

r	read access to the file
w	write access to the file
x	execute access to the file

In a **ls -l** command, the protections are shown as follows:

rwxr-x---

The first three characters are the user's access to the file. The access that is available is read, write, and execute for the user. The next three characters are the group's access to the file. In this example, the group has read and execute access. The last three characters are the access available to other users. In this case, no other users have access to the file.

To change a file's protection, you use the **chmod** (change mode) command. The syntax for **chmod** is:

chmod [u,g,o][+,-,][r,w,x] filename

For example:

```
% chmod o+r test.txt
% chmod g-w temp
```

In the first example, other users are given read access to the file **test.txt**. In the second example, write access is taken away from other users in the group.

Disk Space

Each user is allocated a maximum amount of disk space that he can use for the account. This amount is measured in disk blocks. A block is equal to 512 bytes (1/2 K). All new accounts start with an allocation of 500 blocks or 250K. To see your current disk space usage, type:

% **quota -v**

Sometimes users need more disk space. If you have deleted your unneeded files and you are still do not have enough disk space, contact the UNIX Operators by one of the methods listed at the end of this article.

To keep your disk space usage to a minimum, you can use the **ARC** and

ZOO programs to compress files. See the man topics **ARC** and **ZOO** for more information.

The vi Editor

To access the **vi** editor type **vi** at the % prompt. To exit the editor, type **ZZ** or **:x** or **:wq**.

The Emacs Editor

To access the Emacs editor, type **emacs** at the % prompt. The arrow keys move the cursor one character (or line) in the direction of the arrow. To exit the editor, press **<CTRL>-X <CTRL>-C**

Program Development

Three steps are required to develop a program:

- 1 Create the source program file using the **vi** or Emacs editor. You should use the default file extension for source program files (if any). For instance, if your program is written in **c**, its file type default is **c**.
- 2 Compile or assemble the source program file to produce an object module file. There is a Unix command to invoke each language processor, such as **cc** for **C**.

% **cc prog.c**

By default, this will create an executable file called **a.out**. To select the name of the executable, you need to add the **-o** flag with a filename.

% **cc -o test prog.c**

This command would create an executable file called **test**.

- 3 Finally, run the executable program by typing the filename at the UNIX prompt.

% **test**

Electronic Mail

The Unix **elm** utility allows you to send messages to other users on the same

node or a remote node by means of a wide area network. You can also read, file, forward, delete, print, and reply to messages that other users send to you.

When you log on to the Solbourne, the elm utility will notify you whether you have new messages. To read messages, you need to run the elm utility.

To invoke the elm utility, type elm from the % prompt:

```
% elm
```

Talk Utility

The talk Utility allows users of the Solbourne to talk with other users. In its simplest form, the talk Utility can be invoked by entering talk at the % prompt. This causes the screen to display the phone layout and to await the entry of the username to be called. Upon entry of the username, a message will appear at the top of the screen specifying either that the desired user is not available or that his phone is ringing.

I/O Redirection

Normally, UNIX reads input from the keyboard and sends output to the screen. UNIX allows you to override those defaults and use files as input and output sources. To redirect a command's output to a file, the command should be followed by a > character and the filename. For example:

```
ls file.lst
```

Another type of output redirection allows a command's output to be appended to the end of a file. This option is used in the same way as standard output redirection except instead of using >, the >> symbol is used. For example:

```
ls >> contents
```

Input redirection allows a command to get its input from a file instead of the keyboard. To do this, the command should be followed by a < character and the filename. For example:

```
sort < bnok.txt
```

The final form of I/O redirection is known as pipes. Pipes are a method of redirecting the output of one command to the input of another command. The syntax is to place a | character between the commands. For example:

```
ls | sort
```

Computer Networks

The Solbourne is on several different world-wide and regional computer networks. These computer networks allow users to exchange information with other computer users in other parts of the world. The Computing Center has a handout (in ISB 110 and ISB 119) called "Making Connections" that covers all of the Wide Area Networks that are available.

The Internet is a group of closely related networks containing thousands of computers all primarily based on the TCP/IP protocol. These related networks include MILNET (MILitary NETwork), NSFNET (National Science Foundation NETwork), and CSNET (Computer Science NETwork). The Internet allows users to log into remote computers, transfer files, and send/receive mail. An "Introduction to the Internet" handout is available from the Computing Center in ISB 119.

USENET is a news (mailing list) oriented network that contains much very useful information. USENET is available to Solbourne users through the nn News package.

VAX/Unix Operators

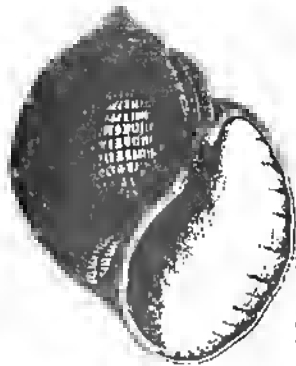
If you have any problems or questions related to the Solbourne, you can call the VAX/Unix Operators at 565-4161. You can also send mail to the operator account on the Solbourne.

More Utilities

Utility	Function
finger	Returns the user information.
news	Lets you see current information on changes, additions, etc. on the VAX and LAN during the last few weeks.
PRT	A menu driven utility that allows users to route files to different printers. ■

D/FW UNIX User's Group

Meetings of the D/FW UNIX User's group are held the first Thursday of every month (unless it is a holiday) at the Hewlett-Packard facility in Las Colinas (3301 Royal Lane, Irving, TX 75063, 214-830-8994). This group is dedicated to "promoting the education and understanding of UNIX." Dues for one year are \$12.00. ■



The UNIX Shell

By Marc St.-Gil, UNIX System Programmer (mstgil@sol.acs.uni.edu)

Hi! My name is Marc St.-Gil and you may have read about me elsewhere in this issue of *Benchmarks*. I have been hired to administer the new Solbourne UNIX system here in UNT's Computing Center. As UNIX is still a mystery to many people, especially new users, I wanted to start a new monthly column in *Benchmarks* devoted specifically to Solbourne UNIX user's here on our campus. Since the Solbourne (sol.acs.uni.edu) is not generally available to the campus yet, I thought I would start out with some very introductory remarks for new UNIX users. All examples used in this column will be specific to the Solbourne, and when I have the time I will research and point out the differences, if any, between usage on the Solbourne and on the other UNIX systems used around campus. First some UNIX conventions:

- Under csh (the C Shell) the '~' character represents your home directory. You may address anyone's home directory with the syntax '~userid' where userid is the account name of the user whose home directory you wish to specify.
- Any file whose name starts with a '.' will not normally show up in the output from an "ls" command, you may think of them as being similar to "hidden files" on a PC.

Setting up a .signature file

All e-mail power-users will want to do this first.

- 1 Create a file ~/.signature with up to 4 lines (max 80 cols. each) containing whatever information you like. Remember that what you put in here will be appended to the bottom of all mail that you send, so make sure it is something everyone will understand. Here is an example:

Marc St.-Gil AKA The Unixmeister
Research Systems Programmer
University of North Texas
PO Box 13495, Denton TX, 76203

mstgil@{sol,vaxb}.acs.uni.edu
mstgil@{ponder,solo}.csci.uni.edu
Academic Computing Services
817/565-2324

- 2 Assuming you use 'elm,' change the lines in ~/.elm/elmrc like:

```
# local ".signature" file to append to appropriate messages...
localsignature =
# remote ".signature" file to append to appropriate messages...
remotesignature =
```

to look like:

```
# local ".signature" file to append to appropriate messages...
localsignature = ~/.signature
# remote ".signature" file to append to appropriate messages...
remotesignature = ~/.signature
```

You can have separate local and remote .sig files if you like, as implied above. Before you ask, local is used for mail going to someone on the Solbourne and remote is used for mail going anywhere else.

Dealing with a file name that has unprintable characters in it

Sooner or later you will accidentally manage to create a file which appears to have a normal name, but you can't seem to delete it (This works on all flavors of UNIX). You'll know this is the problem when a file name shows up in a directory listing, but the rm command insists that the file doesn't exist. Let's say that the listing shows a file called primer.ps\$5nz, and the command 'rm primer.ps\$5nz' doesn't seem to be able to delete the file. The best bet is to try using a wildcard to delete it. If you can 'ls' it using something like 'ls primer*' and you get only the file you want to delete, then you can use the same argument to delete the file. For example:

```
$ ls primer*
primer.ps$5nz
$ rm primer*
$
```

but if:

```
$ ls p*
primer.txt      primer.ps$5nz
$
```

or

```
$ ls primer*
$
```

Continued on page 10; see UNIX Shell.

On-line Bibliographic Data Base Document Updated

By Billy Barron, VAX/UNIX Systems Manager (BITNET: BILLY@UNTVAX)

The latest version of UNT's "Accessing On-line Bibliographic Data Bases" handout is now complete. It now contains 168 library systems covering 220 sites. Credit for most of the new information goes to Dana Noonan, Metro State University (for all the UK info) and Peter Scott, University of Saskatchewan.

Due to the size of this document, we can no longer make it available for general distribution in paper form. A subset of this document, "Accessing On-line Bibliographic Data Bases in the North Texas Area," is available in the Computing Center Reception Area (ISB 119). The complete document is available for reference in the ISB 110, Graphics, Willis, and GAB 5th floor labs. Also, the College of Business (consult the C.O. B. Computer Center) has a copy of this document. Additionally, this document may be acquired by anonymous FTP on VAXB.ACS.UNT.EDU.

How to acquire it via anonymous FTP

```
ftp vaxb.acs.unt.edu
username: anonymous
password: anything-you-want
ftp> get libraries.txt [for ASCII version]

ftp> get libraries.ps [for Postscript version]

ftp> binary
ftp> get libraries.wp5 [WordPerfect 5.1 version]
```

Finally, the files are accessible on the VAX. They reside in the DUAI:[ANON] directory. It is possible to display the ASCII version on your screen with the TYPE command and to download any of the files with Kermit.

Some commonly asked questions

- Are there other files available that are associated with this type of information?

These additional files are available on vaxb.acs.unt.edu (129.120.1.4) via anonymous FTP. They can be obtained as illustrated above.

libraries.adr - Numeric IP addresses of Internet libraries
libraries.contacts - Contacts for some of the Internet libraries
networks.htm - VMS help file source for a wide area networks help topic, which includes a section on library systems.

- Why is there UNT's guide and the Art St. George/Ron Larsen guide?
Art St. George and I have some differences of opinion in the area of formatting and what should be included in an Internet library guide. Joe St. Sauver, the author of the VAXbook, (on PACS-L) put forth a rather good argument for the case that two guides are actually a beneficial thing.
- Are there some other useful sources of information?

- HYTELNET - A Hypertext database for MS-DOS systems on Internet Resources including Library systems. Available via anonymous FTP on WUARCHIVE.WUSTL.EDU, WSMR-SIMTEL20.ARMY.MIL, or VAXB.ACS.UNT.EDU. Written by Peter Scott, University of Saskatchewan. A new version should be released in the near future.

- LIBTEL - A TELNET front-end for VMS and Unix systems to access Library Systems. Available via anonymous FTP on VAXB.ACS.UNT.EDU. Written by D. Mahone, University of New Mexico. I think a new version is in the works also.

- Why don't you use a smaller font size to save paper?

To keep 80 characters or less per line is the major reason. Also, a smaller font will not save that much paper (I've looked at it).

- I have problems printing the PostScript file.

I'm pretty clueless on this one. I have printed the PS file from a PC to an Apple Laserwriter II without a problem. ■

UNIX Shell continued.

you must refine your search:

```
$ ls p*
passwd          primer.ps$5nz
$ ls p*z
primer.ps$5nz
$ rm p*z
$
```

What to do if the system replies "you have stopped jobs" when you try to log out.

If you see that message, it means that you pressed <CTRL/Z> in an interactive application like 'elm'. To restart a stopped job, use the command fg (it stands for ForeGround, which makes sense if you know that stopped jobs are placed in the BackGround). See the Jobs section of the csh man page ('man csh') for more information on this topic. ■

Internet-Accessible BBSs

The following information was posted to LIB HYTELNET by Peter Scott, Order Unit Manager, Univ. of Saskatchewan Libraries, Saskatchewan, Canada (scott@sklib.usask.ca).

I am in the process of compiling information on BBSs accessible via Telnet. I haven't had time to test each one, but can, without hesitation, suggest "dialing-in" to samba.acs.unc.edu if you want to see how a library bbs SHOULD operate. Thanks to Judy Hallman for her fine work. If you want to follow discussions about Internet-accessible BBSs then read the Usenet message area alt.bbs.internet. If you want to know more about IRC, Internet Relay Chat, then read the Usenet message area alt.irc.

Bulletin Board Systems

Name	IP Addr	Login	Description
alf.unomaha.edu		ef	The Endless Forest
atl.calstate.edu		lewisnts	
caticsuf.cati.csufreson.edu		public	Advanced Tech Info Network
fncon1.cwru.edu			Case Western Reserve
freenet-in-a.cwru.edu		—	Cleveland Free-Net; Usenet,IRC
hpcubbs.cv.hp.com		bbs	Hewlett Packard Calculator BBS
isca.icaen.uiowa.edu		iscabbs	U of Iowa - DOC - 1 Gig of D/L
mars.ce.msstate.edu	130.18.64.3	bbs	Full-screen
naval acad. bbs	131.121.161.71	<CR>	Single-user system, so keep trying
quartz.rutgers.edu	128.6.4.8	bbs	Citadel system, very active
samba.acs.unc.edu	128.109.157.30	bbs	XBBS system; U. of N. Carolina
shark.cs.fau.edu	131.91.80.13	bbs	Florida Atlantic U; usenet
star96.nodak.edu	134.129.107.131	20	UnaXcess BBS
toisun.oulu.fi	128.214.5.6	box	Finland; IRC, Usenet
uafcseg.uark.edu	130.184.64.202	bbs	U. of Arkansas; usenet, irc
uvcw.uvic.ca		cosy	U of Victoria, Canada
vtcosy.cns.vt.edu	128.173.5.10	—	Must apply for an account
	130.18.80.10	dawg	Mississippi State U.
	35.1.1.6	um-m-net	Michigan
	35.1.1.6	um-interconnect	Michigan

Mailing Binary Files

This article is a combination of two separate articles. Portions are excerpted from an article by the same name that appeared in the February 1991 issue of the Buffer, the newsjournal of computing at the University of Denver. That article is by Bob Stocker, Director of Academic Computing at the University of Denver (BITNET: BSTOCKER@DUCAIR). Portions of this article are also reproduced from a Micro-Tip, "Transferring Data Overseas," that appeared in the October 1990 issue of Benchmarks.

You may have been told by someone that you can't mail binary files. That's not true, but its not completely untrue.

Some examples of binary files are: executable programs, documents created by a word processor like WordPerfect, worksheet files created by spreadsheet programs, and graphics images. These files almost always contain special characters that will cause an electronic mail system to choke and gag. If anything at all comes out at the other end, it won't be the same thing that you put in.

The problem is that mail systems are designed to handle "plain-text" files that contain only printing characters like letters, digits, and punctuation marks and a few special characters that indicate things like the ends of lines and page breaks. These files are also called "ASCII" files.

On most computers characters are stored in eight-bit fields called bytes. Plain-text characters represent only about half of the 256 characters that can be stored in a byte.

Electronic mail systems have trouble with the 128+ "non-plain-text" characters that appear in binary files. Some systems, like VMSmail, also have

problems with lines that are longer than one would expect to find in a plain-text file. Other mail systems have trouble handling files that are larger than some arbitrary size.

The way to get around the problem is to translate binary characters to plain-text characters. Because plain-text characters can also occur in binary files, this requires a little sleight of hand.

The trick is to use four bytes of plain text (32 bits) to represent three bytes (24 bits) worth of binary data. In this scheme, each six-bit field in the 24 bits of binary data is represented by an eight-bit character. Only 64 characters (enough to represent each possible value that can be stored in six bits) are required to do the job.

Once that's done, the rest is easy. A few special characters need to be inserted to break the file up into lines that are short enough to satisfy programs like VMSmail, and the file itself has to be broken up into sections that are small enough to be mailed.

Enough of bits and bytes. There is a standard way of doing all this.

Preparing binary files on your Macintosh for sending via electronic mail. For the Macintosh, the BinHex format is commonly used to encode binary files in ASCII form for mailing. Freely distributable programs, such as Stuffit or BinHex 4.0, can be used to convert your files to this format. These same programs are used on the receiving end to convert the files back to usable form. Stuffit and BinHex 4.0 are available in the Computing Center Graphics Lab (ISB 6).

Preparing binary files on your DOS PC for sending via electronic mail. For MS-Dos and PC-Dos machines, there are freely distributable programs that use the "uuencode" format to translate binary files to an ASCII form that can be sent via electronic mail. The

Continued on page 14.

THE BITNET CONNECTION

By Dr. Philip Baczewski, BITNET INFOREP (BITNET: AC12@UNTVM1)

*This Column is a continuing feature of **Benchmarks** intended to present news and information on various aspects of the BITNET wide area network.*

How Can I sign onto BITNET?

That used to be one of the more common questions asked about BITNET. These days, however, most people know that BITNET is not something that you sign onto, but rather a system to carry information between host computers. Still, there are a number of questions about using BITNET that are asked on a regular basis. In this month's column, I'll answer five of the most frequently asked questions about BITNET. The first envelope, please...

*I'm trying to send mail to **HOMER@SUSHI.STANFORD.EDU** from **MUSIC**, but my mail gets returned with a message saying "undeliverable mail." Can I send mail to that address from **MUSIC**?*

Unfortunately, no. The address given above is actually an Internet address which must pass through a gateway from BITNET to the Internet in order to reach its destination. While MUSIC users can send mail and files to all addresses that are part of BITNET or its associated networks, because of technical limitations in MUSIC and its mail programs, mail service to networks via gateways is not available to MUSIC users. BITNET addresses will always have userid and node portions that do not exceed eight characters. If you regularly need to send mail to Internet or other "gatewayed" addresses, you may wish to add CMS or VAX access to your userid; both of those systems are better equipped to handle BITNET and Inter-network mail.¹

How do I subscribe to a BITNET mailing list?

The same basic command can be used to subscribe to any BITNET mailing list: **SUB <listame> <your name>** where SUB stands for "subscribe," <listame> is the name of the mailing list, and <your name> is your first and last name. You don't have to specify your BITNET address, since it is automatically contained in the message you will send to subscribe. The tricky part is knowing how and where to send this command.

First the "how" part: the subscribe command can be sent as an interactive message from the VAX or CMS, and can be sent as the first line of a mail message from any system connected to BITNET. Now the "where" part: most BITNET mailing lists are referred to in the form of a BITNET address with the format <listame> @<node>. Since mailing lists are almost always maintained by a LISTSERV installation, your *subscribe* command should be sent to **LISTSERV@<node>**,

¹ For more information on mail gateways, see "The BITNET Connection" in the February, 1991 issue of *Benchmarks*.

where **LISTSERV** is the userid portion of the BITNET address and **<node>** is the node found as part of the list specification. Sometimes, you only know the list name and not its associated node. All is not lost, however, since most **LISTSERVs** on BITNET know about all other **LISTSERVs** and the mailing lists they maintain. This means that you can send your *subscribe* command to the nearest **LISTSERV** and it will forward your request to the appropriate installation (the closest **LISTSERV** to UNT is **LISTSERV@UTDALVM1**). So, to subscribe to a mailing list (all entries go on one line):

- From the VAX, type:

```
SEND LISTSERV@<node> SUB  
      <listname> <your name>
```

- From CMS, type:

```
TELL LISTSERV@<node> SUB  
      <listname> <your name>
```

- Or, on MUSIC, CMS, or the VAX, send a mail message to:

LISTSERV@<node> with the line **SUB <listname> <your name>** as the first line of the mail message.²

How do I sign off of a BITNET mailing list?

The command to stop a BITNET **LISTSERV** subscription is **SIGNOFF <listname>**. This command must be sent to the appropriate **LISTSERV** (see above) via either an interactive message or as the first line of a mail message. If you are going to be away and unable to read your BITNET mail for any length of time, it is a good idea to sign off of all of your BITNET mailing list subscriptions. This can be accomplished with one command sent to the nearest **LISTSERV**: **SIGNOFF *** (**NETWIDE** meaning, sign off of all

² For more information on BITNET mailing lists and **LISTSERV**, see "The BITNET Connection" in the May/June 1989 issue of *Benchmarks*, or see "An Introduction to BITNET," available from the Computing Center offices (ISB 119).

LIST of the Month

*Each month we will highlight one of the BITNET **LISTSERV** Special Interest Group (SIG) mailing lists. This month's list...*

AIX-L@BUACCA

Coordinator: Michael Gettes (**CCMRG@BUACCA**)

IBM AIX Discussion List is intended for the discussion of AIX. AIX is the IBM Unix solution for small and large computer systems. Initially, this list will be used for dissemination of information and technical details of AIX on all levels. It may be necessary to break this list down into machine types that AIX will run on.

*This list is specific to the IBM version of Unix, only. To subscribe, send the following command to **LISTSERV@BUACCA**:*

```
SUB AIX-L <your name>
```

Also of interest may be the following Unix-related USENET discussion lists maintained in ANU NEWS on the VAX:

comp.unix.aix	comp.unix.amiga	comp.unix.aux
comp.unix.internals	comp.unix.large	comp.unix.misc
comp.unix.msos	comp.unix.programmer	comp.unix.questions
comp.unix.shell	comp.unix.sysv286	comp.unix.sysv386
comp.unix.ultrix	comp.unix.wizards	comp.unix.xenix.misc
comp.unix.xenix.sco		

comp.unix.questions and comp.unix.wizards are two of the most active of these lists. The first handles novice and beginner questions, while the second handles complex issues like system installation and configuration.

mailings lists subscribed to, anywhere on BITNET. However, since this command generates a large number of messages on BITNET, if you are subscribed to only one or two lists, it is best to send *signoff* messages directly to the

LISTSERVs where your subscriptions are maintained.

How can I find out the BITNET address of someone at another BITNET node?

General Information

There is no central directory of BITNET users, however, there are a number of methods to finding out other people's BITNET addresses, none of which are guaranteed to work. A number of directory servers exist on BITNET, where people can register their BITNET addresses.³ Also, a number of LISTSERV installations support a /WHOIS <name> command which can be sent to find out the name of someone subscribed to a mailing list at that installation. Both of these methods are extremely "hit-or-miss," since there is no assurance that the person that you are seeking will be registered or subscribed on the server to which you are inquiring. Most nodes have a "postmaster" userid (usually POSTMAST@<node>), and you can try sending a polite inquiry as to someone's address to that userid. If that doesn't work, you can try a similar message to that site's BITNET Inforep (the person at a node responsible for providing information on BITNET; in UNT's case, me). To find out the address of an Inforep for a particular node, send the following command to the closest NETSERV (for UNT, NETSERV@UTARL.VMI): GET NODENTRY <node>. You will receive a file with several pieces of information, including an entry which is similar to following:

:inforep.(name) userid@node

The address following the :inforep "tag" is the address to which you want to send your inquiry.

When I try to send mail to the address b1234@uk.ac.oxford.english the mail gets returned with an "undeliverable mail" message. Can I send mail to this address?

This type of address structure indicates a node on the United Kingdom research network called *Janet*. You can send mail to *Janet* from CMS or the VAX, but you must "reverse" all the portions of the node specification so that the "uk" part is last. To send to the example above, you would use b1234@english.oxford.ac.uk as the address.

How can I sign onto BITNET?

Now, I thought we'd been over that already.... ■

³ For a list of directory servers and help in using them, see "The BITNET Connection," in the October 1989 issue of Benchmarks, or refer to "An Introduction to BITNET," available at the Computing Center Offices (ISB 119)

Staff Activities

- Dave Molta, Director of Academic Computing, attended a NetWorld 91 Advisory Board planning session in Orlando, FL, on January 18, where he was selected as a track chair for the *NetWorld Dallas* conference, to be held in October. He also conducted a full-day tutorial on the TCP/IP Protocol Suite at the Communication Networks conference in Washington on January 28. Finally, Molta served as moderator for a seminar on "LANs in Education" at the *NetWorld Boston* conference on February 14.
- Dr. Philip Baczewski, Academic Mainframe User Services Manager and Panu Sittiwong, Academic Statistical Consultant, attended the SAS Users Group Meeting (SUGI) in New Orleans February 16-20. ■

Binary continued from page 12.

same program, or sometimes a separate "uudecode" program, is run on the destination PC to convert the files back to a usable form. XXENCODE, which performs both of these functions, is available from the BBS on the VAXcluster in the IBM.Utility area.

Mailing the file. In order to mail a file via BITNET or the Internet, you will need to move the file to your host account using a file transfer program such as Kermit or ftp. You can make additional changes to the format of plain text files on the host, but don't change encoded files.

Encoded files consist only of printable characters, but contain no information that makes them recognizable to people. When you send encoded binary files, include a header that indicates exactly what is being sent, but clearly delineates the header from the file itself. A standard way to do this is to put lines such as the following before the file:

The following Microsoft Word 4.0 file was encoded in BinHex 4.0 format using Stuffit

-----Cut Here-----

Mailing files from CMS. To mail an encoded file from CMS it is preferable to use the MAIL command. (The SENDFILE command may alter the file in a way that will make it impossible to decode.) The command MAIL <dest id> (FILE <CMS filename>) will invoke the mail program and include the specified CMS file as the mail text. PF5 will send the message. Type HELP MAIL for more information.

Mailing files from VAX/VMS. To mail a file from VMS, type MAIL and then, at the MAIL> prompt, type SEND and the file name.

Mailing files from MUSIC/SP. To mail an encoded file from MUSIC, type MAIL and proceed as you normally would to send a message, however put the name of the encoded file in the

General Information

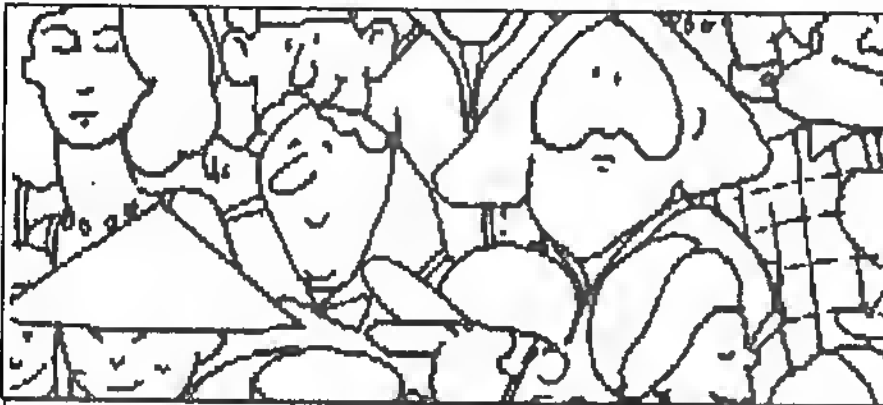
"input file" field. Continue sending your mail in the usual manner.

Mailing files from UNIX. On UNIX, use the mail command to send your file. You can add comments and files to a message by using ~v or ~r commands within mail. For explanations of these commands, type ~? at the start of a line while entering your mail message.

Receiving files. On the receiving end, the file is delivered as electronic mail to the recipient's electronic mail account. The headers should be deleted before an encoded file is downloaded to a personal computer from a mail account on a mainframe. The recipient then runs the corresponding decoding program on the personal computer.

Caveat. The most common encoding programs produce files that can be sent reliably over the Internet but may become garbled in some parts of BITNET. If you experience difficulty transferring files in this way, contact Academic Computing Services (565-2324).

This may sound complicated, but it allows for very fast and reliable transfer of files with formatting intact to many places in the world. ■



BENCHMARKS FORUM

BENCHMARKS FORUM is intended to serve as a vehicle for answering questions that may be of general interest to the user community. If you have a question, please send electronic mail to the Benchmarks editor (BITNET: AS04@UNTVMI) or write it down and drop it by the Computing Center. We will try to answer it in the next issue.

Question: What is TCP/IP?

Answer: TCP/IP (Transmission Control Protocol/Internet Protocol) is the common name for a family of data-communications protocols used to tie computers and data-communications equipment into computer networks. TCP/IP originated for use on a network called ARPANET, but it is currently used on a large international network of universities, other research institutions, government facilities, and some corporations called the Internet. TCP/IP is also sometimes used for other networks, particularly local area networks that tie together numerous different kinds of computers or tie together engineering workstations.

Question: What is "The NIC"?

Answer: "The NIC" is the Defense Data Network, Network Information Center (DDN NIC) at SRI International, which is a network information center which holds a primary repository for RFCs and Internet drafts. The host name is NIC.DDN.MIL. Shadow copies of the RFCs and the Internet Drafts are maintained by the NSFnet on NNSC.NSF.NET and on MERIT.EDU.

In addition, the DDN NIC is the Internet registration authority for the root domain and several top and second level domains; maintains the official DoD Internet Host Table; is the site of the Internet Registry (IR); and maintains the whois database of network users, hosts, domains, networks, and Points of Contact.

Question: How do I find someone's electronic mail address?

Answer: There are a number of directories on the Internet; however, all of them are far from complete. The two largest directories are the WHOIS database at the DDN NIC and the PSInet White Pages. Generally, it is still necessary to ask the person for his or her email address.

Question: How do I use the WHOIS program at the DDN NIC?

Answer: To use the WHOIS program to search the WHOIS database at the DDN NIC, telnet to the NIC host, NIC.DDN.MIL. There is no need to login. Type "whois" to call up the information retrieval program. Next, type the name of the person, host, domain, network, or mailbox for which you need information. If you are only typing part of the name, end your search string with a period. Type "help" for a more in-depth explanation of what you can search for and how you can search.

Question: How do I become registered in the DDN NIC's WHOIS database?

Answer: If you would like to be listed in the WHOIS database, you must have an electronic mailbox accessible from the Internet. First obtain the file NETINFO:USER-TEMPLATE.TXT.

General Information

You can either retrieve this file via anonymous FTP from NIC.DDN.MIL or get it through electronic mail. To obtain the file via electronic mail, send a message to SERVICE@NIC.DDN.MIL and put the file name in the subject line of the message; that is, "Subject: NETINFO USER-TEMPLATE.TXT". The file will be returned to you over night.

Fill out the name and address information requested in the file and return it to REGISTRAR@NIC.DDN.MIL. Your application will be processed and you will be added to the database. Unless you are an official Point of Contact for a network entity registered at the DDN NIC, the DDN NIC will not regularly poll you for updates, so you should remember to send corrections to your information as your contact data changes.

Question: How do I use the White Pages at PSI?

Answer: Performance Systems International, Inc. (PSI), sponsors a White Pages Pilot Project that collects personnel information from member organizations into a database and provides online access to that data. This effort is based on the OSI X.500 Directory standard.

To access the data, telnet to WP.PSI.COM and login as "fred" (no password is necessary). You may now look up information on participating organizations. The program provides help on usage. For example, typing "help" will show you a list of commands, "manual" will give detailed documentation, and "whois" will provide information regarding how to find references to people. For a list of the organizations that are participating in the pilot project by providing information regarding their members, type "whois -org *".

For more information, send a message to INFO@PSI.COM.

Question: What is anonymous FTP?

Answer: Anonymous FTP is a conventional way of allowing you to sign on to a computer on the Internet and copy specified public files from it. Some sites offer anonymous FTP to distribute software and various kinds of information. You use it like any FTP, but the username is "anonymous" and the password is "guest" (many organizations request that you use your local userid as a password, for tracking purposes — example: AS04@UNTVM1).

The above questions and answers are from the document RFC1177 ("FYI on Questions and Answers to Commonly asked 'New Internet User' Questions") by G. Malkin, A. Marine, and J. Reynolds. It is available via Anonymous FTP on NIC.DDN.MIL

The following questions and answers come from the article "UNIXland/Netland" by Robert Felts that appeared in the February, 1991 Metroplex UNIX Users Group Newsletter.

Question: What is the Internet?

Answer: An internet is a combination of many smaller sub-nets, basically a network of networks. The Internet (with a capital I) is a large internet that connects many sub-nets around the world and is primarily available for research. Most of the sub-nets are TCP/IP based, but not necessarily.

The Internet was previously known as the ARPAnet. As research groups began to add sub-nets to the ARPAnet it began to be more and more research oriented. Over time the Defense network became controlled by NSFnet. And is now referred to as the Internet.

Question: What is UUCP?

Answer: UNIX to UNIX CoPy is a network application. It is a sub-system of UNIX that allows remote file copying and remote job execution across different media. The original and primary media is dial-up phone lines. T1, T3 lines, TCP/IP LANs and the Internet are used. UUCP has been ported to VAX/VMS and PC/MS-DOS. The UUCP "Network" really

doesn't exist as a network, but if you insist that it does, it consists of all the sitex and transmission media used by those sites.

Question: What is the USENET?

Answer: USENET is a collection of application programs used to broadcast data to multiple sites. It facilitates the posting of messages to specific newsgroups, the indexing and storage of messages received from other machines. It administers news handling. It can operate over UUCP or Internet.

Question: What is the UUNET?

Answer: UUNET is a company which provides services to their subscribers. These services include running a UUCP site called UUNET, and acting as an internet forwarder via their internet gateway, uunet.uu.net. Each UUCP site which connects to UUNET pays for their connect time. There are other sites besides UUNET which act as gateways between the UUCP network and the Internet, including Apple, Atina, Cornell, cs.utexas.edu, decuac, gatech, Harvard, and Mcsun. According to their UUCP map entry UUNET is:

UUNET Communications Services
3110 Fairview Park Drive, Suite 570
Falls Church, VA 22042-4239

Latitude-Longitude: 38 51 N / 77 12 00 W

Email: uunet!postmaster or
postmaster@uunet.uu.net
Telephone: + 1 703 876 5050

As UUNET's services are for their paying subscribers, you should have permission from one of these subscriber sites to send mail through UUNET. Many of UUNET's subscribers allow mail to be forwarded through them, as long as this courtesy is not abused.

Question: What are some other sources of information about the Internet, USENET, UUNET, and UUCP?

General Information

Answer: The following books discuss these topics. Most are available at Taylor's Technical Bookstore or The Book Stop.

Title: *Life With UNIX*
Author: Libes, Don & Ressler, Sandy
Publisher: Prentice Hall
Pages: 350
ISBN: 0-13-536657-7
Cost: \$30.95
Summary: It answers all the puzzling questions that seem to be between the lines of every other book. For example, there is a chapter "UNIX Underground" that describes UUCP, USENET, UUNET, the Internet, newsgroups, mailing lists, FSP, Minix Xinu, etc., their relationship to each other and other things. The book includes addresses for everything mentioned.

Title: *UNIX Communications*
Author: Waite Group (authors Anderson, Costales, Henderson)
Publisher: The Waite Group via Howard W. Sams
Pages: 542
ISBN: 0-672-22511-5
Cost: \$26.95
Summary: Covers everything the end user needs to know about email, USENET, and UUCP.

Title: *Using UUCP and USENET*
Author: Todino, Grace
Publisher: O'Reilly & Associates, Inc.
Pages: 91
ISBN: 0-937175-010-2
Cost: \$17.95
Summary: A good guide to the UUCP and USENET world.

Title: *Managing UUCP and USENET*
Author: O'Reilly, Tim & Todino, Grace
Publisher: O'Reilly & Associates, Inc.
Pages: 107
ISBN: 0-937175-09-9
Cost: \$21.95
Summary: A big help to System Administrators working, setting up, and maintaining UUCP and USENET.

Title: *!%@::A Directory of Electronic mail Addressing and Networks*
Author: Fey, Donnalyn & Adams, Rick
Publisher: O'Reilly & Associates, Inc.
Pages: 284
ISBN: 0-937175-93-0
Cost: \$26.95
Summary: Explains the email and network world. ■

Benchmarks Reader/User feedback is encouraged. Send all letters, suggestions, etc to (AS04@ UNTVM1), FAX 817-565-4060 or to the Benchmarks Editor at:

**Academic Computing Services
University of N. Texas Computing Center
P.O. Box 13495
Denton, Texas 76203**



OS/MVS JCL Utilities: IEBCOMPR

By Cathy Hardy, Academic Database Consultant (BITNET: AC55@UNTVM1)

This is the fourth in a series of articles dealing with JCL (job control language). This series is aimed at the current JCL user who would like to have a better understanding of statement use, utilities, and coding options. If you are not currently a JCL user, but would like to begin learning about JCL, Academic Computing has a free handout available in ISB 119. Stop by and ask for "IBM Job Control Language," or contact an Academic Mainframe Users Support consultant for further information.

IBM Utilities

There are three classes of utility programs:

- ① **system**, used to maintain and manipulate system and user data sets,
- ② **independent**, used to prepare devices for system use when the system is not available, and
- ③ **data set**, used to reorganize, change, or compare data sets at the data set or record level.

As a programmer, you will generally be interested in the data set utilities.

Data Set Utilities

Data set utilities are used to manipulate partitioned, sequential, or indexed data sets. Data being manipulated can range from fields within a record to entire data sets. There are nine data set utilities:

- ① **IEBCOMPR** - compares records in sequential or partitioned data sets.
- ② **IEBCOPY** - copies, compresses, or merges partitioned data sets; renames and/or replaces member of partitioned data sets.
- ③ **IEBDG** - creates test data sets.
- ④ **IEBEDIT** - selectively copies job steps and JOB statements

General Information

- ⑤ IEBGENER - copies records from a sequential data set or converts a data set from sequential to partitioned organization
- ⑥ IEBISAM - copies ISAM files
- ⑦ IEBPTPCH - prints (or punches) records in sequential or partitioned data sets
- ⑧ IEBTCRIN - used to construct records read from Tape Cartridge Readers
- ⑨ IEBUPDTE - incorporates changes to sequential or partitioned data sets

IEBCOMPR

IEBCDMPR is an IBM data set utility which will compare two sequential or two partitioned data sets, record by record. It is primarily used to verify backup copies. IEBCOMPR can compare fixed, variable, or undefined records from blocked or unblocked data sets.

Sequential data sets are considered to be 'equal' if they have the same number of records and their corresponding keys and records are identical. If the two data sets don't meet these requirements, an 'unequal' comparison will be made. If the records are not equal the record and block numbers, the names of the DD statements that define the data sets, and the unequal records are listed. Ten successive unequal comparisons will terminate the job step.

Partitioned data sets are considered 'equal' if the members contain the same number of records, lists are in the same position within corresponding members, and corresponding keys and records are identical. If these requirements are not met, an 'unequal' comparison will be made. After ten successive unequal comparisons are made, processing will continue with the next member.

If Directory-One has members A, B, C, D, and E, and Directory-B has members A and D, only members A and D will be compared. If Directory-A and B have no common members, the compare will terminate abnormally.

Example JCL for IEBCOMPR (Partitioned data sets):

```
//JOB CARD
//STEP1 EXEC PGM=IEBCDMPR
//SYSPRINT DD SYSOUT=A
//SYSUT1 DD DSN=PDSSET1,UNIT=SYSDA,DISP=SHR,
//   DCB=(RECFM=FB,LRECL=80,BLKSIZE=800),
//   VOL=SER=ACAD01
//SYSUT2 DD DSN=PDSSET2,UNIT=SYSDA,DISP=SHR,
//   DCB=(RECFM=FB,LRECL=80,BLKSIZE=800),
//   VOL=SER=ACAD01
//SYSIN DD *
//   COMPARE TYPORG=PO
/*
//
```

The control card (SYSIN) specifies the type of organization of the input data set (partitioned (PO), sequential (PS)).

For additional information on IBM utilities, check your IBM OS/VS2 MVS Utilities manual. Next issue: IEBCOPY ■

Spring Break Lab Hours

Following are the Spring Break hours for the listed facilities:

Computing Center RJE

- Saturday, March 9: Close at Midnight
- Sunday, March 10: Noon - Midnight
- Monday-Saturday, March 11-16: 8 a.m. - Midnight
- Sunday, March 17: Noon - Midnight

ISB IIO Lab

- Saturday, March 9: 9 a.m. - 8:50 p.m.
- Sunday, March 10: CLOSED
- Monday-Friday, March 11-15: Noon - 11:50 p.m.
- Saturday, March 16: CLOSED
- Sunday, March 17: 2 - 11:50 p.m.

College of Business

- Friday, March 8: 8:15 a.m. - 4 p.m.
- Saturday, Sunday March 9 & 10: CLOSED
- Monday-Friday, March 11-15: 10 a.m. - 6 p.m.
- Saturday, March 16: 8:15 a.m. - 7:45 p.m.
- Sunday, March 17: Noon - Midnight

GAB 550

- Saturday-Saturday, March 9-16: CLOSED
- Sunday, March 17: 2 p.m. - Midnight

Graphics Lab

- Saturday, Sunday March 9, 10: CLOSED
- Monday-Friday, March 11-15: 8 a.m. - 5 p.m.
- Saturday, March 16: CLOSED
- Sunday, March 17: 1 p.m. - Midnight

Willis Library Lab

- Saturday, March 9: 9 a.m. - 9 p.m.
- Sunday, March 10: CLOSED
- Monday-Friday, March 11-15: 8 a.m. - 5 p.m.
- Saturday, March 16: CLOSED
- Sunday, March 17: 1 p.m. - Midnight

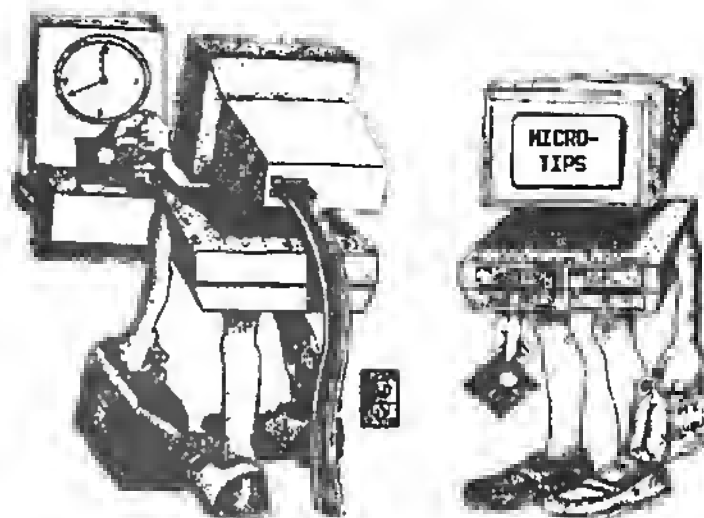


Some PC Viruses Described

The following PC viruses (217 - Number of the Beast, this time) are described by Fridrik Skulason, author of the shareware antiviral program F-PROT (frisk@rhi.hi.is). These descriptions are as of January 1991 and were distributed with F-PROT 1.14. [There's some good material here for social science research — ed.]

- **217** — This is a small, not very interesting virus from Poland, which only infects .COM files.
- **405** — Unlike most other program viruses, this one will not increase the length of infected programs (unless they are shorter than 405 bytes). It will overwrite the first 405 bytes in the files it infects. As this primitive method causes the destruction of many programs, the virus is easily found, and therefore not a serious threat. The "405" virus will only infect .COM files, but it is unable to recognize a file already infected.
- **417** — This is a simple 417 byte virus from Eastern Europe. The only text message inside the virus are the words "F— You". The virus has not been fully analyzed yet.
- **440** — A 440 byte, direct-action .COM infecting virus. Awaiting analysis.
- **492** — This virus from eastern Europe would not be remarkable, if it was not for the fact that it will not work on the 8088 or 8086 processor. The reason is the use of an instruction (PUSH-immediate) which only exist of later-generation processors. The virus only infects .COM files.
- **516** — This simple, Russian .COM virus is interesting in one way - it is

Continued on page 20.



This column is intended to serve as a forum for sharing useful tips on making more productive use of microcomputers. If you have a tip that you feel may be of use to campus users, submit it to the Benchmarks editor for possible inclusion in a future issue.

Allowing Others Access to Your WP Office Mail

This Micro-Tip was supplied by Kyle Capps, Academic Computing Services Microcomputer Support Manager.

Several WP Office mail users have asked if it is possible to grant access to personal mail boxes so that any mail messages may be previewed or printed by another mail user. This feature is available in Office Mail and I have outlined the necessary procedures required to grant access to your mail box.

You cannot grant access to your mail box without invoking the password security feature available within WP Mail.

Procedure to Activate Password Protection

To activate the password protection:

- Get into WP Mail.
- At the main mail screen (both IN and OUT boxes are displayed) press <SHIFT+F1> to invoke SETUP. Four menu options will be available on the screen.
- Press <4> to modify the Environment settings. Three more menu options will appear on the screen.
- Press <3> to select Password. Two prompts will appear at the bottom of the screen: "1: Set Password ; 2: Remove Password".
- Select **1** to establish the password for mail. You will be required to type your password twice for confirmation.
- After entering your password, press <ENTER> or <F7> to exit the SETUP routine. Your mail boxes are now configured to allow access by other mail users.

Accessing Other People's Mail Boxes

To access another person's mail box, you must make certain modifications to your Shell menu. Follow the procedures outlined below to configure the Mail menu item:

- ① At the WordPerfect Office Menu, press <4> for Setup.
- ② Move the highlight bar to the WP Office Mail menu title.
- ③ Press <ENTER> to modify the menu selection.
- ④ Press <ENTER> to move between input fields until the cursor is at the input field for "Prompt For Startup Options".
- ⑤ Press <Y> to change the field value to YES.
- ⑥ Press <F7> twice to exit the Setup function.

These modifications allow you to pass various startup options to the mail system whenever you invoke mail. Upon starting mail, the system will prompt you for any startup options at the bottom of the screen. To access another mail box, enter /@u-<MAIL ID>. <MAIL ID> is the WP Office Mail ID of the individual that has granted access to their mail box. Example: /@u-SMITH. Upon loading mail, you will be requested to enter the password established by the owner of the mailbox. Once entered correctly, you will have full access to their In/Out mail boxes.

If the you press <ENTER> without entering any startup options, WP Mail will default to the current user.

If you are executing Mail from the DOS command line, enter the following command to access other mail boxes:

ML./@u-<MAIL ID>

If you try to access any mail boxes without obtaining access, the message "ACCESS DENIED" will appear and you will be refused access to the mail boxes.

Procedure to Remove Access to the Mail Boxes

To remove access to your mail box, simply remove password protection. This is accomplished by following the procedures for activating the password protection, outlined on page 19, with the exception of responding with a "2" instead of a "1" when given the option of "1. Set Password 2. Remove Password".

Allowing others access to your mail can be very useful, however be aware that anyone with your WP Mail password can send, view, and delete any or all of your mail. For this reason, be very careful in utilizing this feature and never set a password in WP Mail that is identical to passwords on other computer systems you have authorization to access. ■

Viruses continued from page 19

the first virus which does not modify the beginning of the programs it infects. The virus code is located at the end of infected programs, but the jump to the virus is inside the program, not at the beginning, as is usual.

- 696 — This is a simple direct-action Russian .COM virus, which has not been analysed yet.
- 699 — This virus adds 699 bytes to the files it infects, but in addition it may add several "garbage" bytes. As a result disinfected files will often not be of exactly the same length as the original file.
- 707 — This a Russian, 707 byte COM virus, which is awaiting analysis.
- 948 — This Russian virus seems related to the Yankee virus. It infects .EXE and .COM files, including COMMAND.COM, which is infected by overwriting, and should be replaced if infected.
- 1075 — This Russian virus does not seem to work on the 8088 IBM-PC I use for testing viruses - infected programs simply hang the machine. The virus seems to be able to infect .EXE and .COM files, but has not been analysed yet.
- 1260 — This virus is based on the Vienna virus, but the author, Mark Washburn, has made considerable modifications to it. The most significant change is that the virus is now encrypted. As the name indicates, the virus adds 1260 bytes to the files it infects. The first 39 bytes contain a simple decryption routine, similar to the one used by the Cascade virus. There is one important difference, however. A variable number of short (1- or 2-byte) instructions are added between the decoding instructions. The extra instructions do not affect the operation of the virus - they are only placed there in an attempt to prevent virus scanners from using identification strings. This makes it a little harder to detect the virus, but

DrawPerfect Demo to be Featured at WordPerfect Users Group Meeting

Jack Reeve, the Regional Manager of WordPerfect Corporation in this area will give a demonstration of DrawPerfect at the March 22 WordPerfect Users Group Meeting. The meeting will be held from 2-4 p.m. in Room 105 of Marquis Hall (the Training Lab). All interested persons are invited to attend. ■

F-FCHK is nevertheless able to do it. Another variant of the virus exists. It is named Casper because of the following text which is found inside the virus.

Hi! I'm Casper The Virus,
And On April The 1st I'm
Gonna F— Up Your Hard
Disk REAL BAD! In Fact I
Might Just Be Impossible To
Recover! How's That Grab
Ya! GRIN

The virus will indeed activate on April 1st and try to format the boot sector, with incorrect parameters. The code seems to contain an error, though.

The author of the I260 virus, Mark Washburn, has also written and distributed the V2P2 virus, which is somewhat longer than I260 virus.

His last virus, V2P6 is still longer, and uses a much more complex self-modifying encryption method. F-FCHK will detect the virus, but can not remove it. If your system ever gets infected by this virus, I suggest you contact the author and demand a disinfection program from him. His address is:

Mark Washburn
4656 Polk Street NE
Columbia Heights, MN
55421 USA

- **1600** — According to reports from Bulgaria, the author of this virus is the same as the one who wrote the Nina virus, and inside the I600 virus the following message can be found:

Dear Nina, you make me
write this virus; Happy new
year!

The 1600 virus infects .EXE and .COM files, increasing their length by 1600 bytes, but COM-MAND.COM is overwritten. At least some versions of COM-MAND.COM will not work if infected, and infected COM-MAND.COM files should be replaced, not disinfected.

- **2144** — This Russian virus appears to be related to the Voronezh virus -

perhaps having the same author. It is an encrypted .COM and .EXE infector, which has not been fully analyzed yet, but is reported to have a similar effect as the Sverdlov virus.

- **2480** — This virus is not a serious threat on most systems, as it only spreads if the year is set to 1988. It was found in Finland, and has not yet been reported elsewhere. It only infects .COM files, and as the name indicates, it is 2480 bytes long.
- **5120** — This is one of the largest viruses known, 5120 bytes. It will infect both .COM and .EXE files, selecting one file of each type to infect, when an infected program is run. Parts of the virus seem to have been written in a high-level language, probably compiled BASIC, but the initialization code is written in assembly language.
- **800** — One of the Bulgarian viruses - 800 bytes long. It bears some resemblance to the Dark Avenger. It seems to overwrite directories, but has not been fully dissected yet.
- **8-tunes** — Just as most other "music" viruses, this one is from Germany. It infects .COM files as well as .EXE files. When it activates it will play one out of 8 different tunes. The length of the virus code is 1971 bytes.
- **Agiplan** — This virus was first reported in the German AGIPLAN company, but then it disappeared for nearly two years, until a sample appeared in South Africa. Structurally the virus is similar to the Zero Bug virus, as both add 1536 bytes to the beginning of the programs they infect. The virus will not have any serious effects until it has been active on an infected machine for several months, but then it will start corrupting writes.
- **AIDS** — This is a long virus, over 12K, written in Pascal, which overwrites the files it infects. It is therefore easily detected, and not a serious threat.

- **AIDS-2** — This is a "companion" virus, in the form of a .COM file, which will locate a .EXE file and create a corresponding .COM file, exploiting the fact that DOS will first execute the .COM file, containing the virus. The virus will then later execute the .EXE file.
- **Alabama** — This virus was first reported in Israel, but a text string inside it says:

SOFTWARE COPIES
PROHIBITED BY
INTERNATIONAL
LAW..... Box 1055
Tuscumbia ALABAMA
USA.

This message will also appear on the screen in a box on the screen one hour after an infected program is run.

Like a few other viruses this one cannot be removed from memory by pressing Ctrl-Alt-Del. It will simply fake a "reboot" and remain in RAM.

Alabama will only infect .EXE files, increasing their size by 1560 bytes.

Unlike most other resident viruses, it will not automatically infect every new program executed. When a program is run, Alabama will instead search for some other program to infect - probably so the program being executed will get the blame. It will only be infected if no uninfected file is found in the current directory.

Every Friday the virus will do something odd. It searches for a file to infect as described above, and executes it instead of the file the user was planning to execute. A bit weird ...!

One variant of this virus, Alabama-B is also known. It has been distributed in the form of a modified SDIR.COM file, but normally Alabama will not infect .COM files.

- **Ambulance** — As the name indicates, the ambulance virus displays an ambulance on the screen. It is a

796 byte .COM infecting virus. A related virus, 1067 byte long is also known, but it has not been analyzed yet.

- **Amoeba** — This is a 1392 byte .EXE and .COM infecting virus, but little is yet known about it. It overwrites the first 1089 bytes of .COM files, placing the original code at the end and then it appends another 303 bytes. The name of the virus is derived from the following text found inside it.

SMA KHETAPUNK -
Nouvel Band A.M.O.E.B.A

The virus was first reported in Indonesia.

- **Amstrad/Pixel** — This virus is rather interesting. It is a direct-action virus, that will add 847 bytes to the front of any .COM file it finds in the current directory. The virus code is only around 334 bytes, which made it for a while one of the shortest PC virus known. The rest contains zeros and an advertisement for Amstrad computers which is occasionally displayed. Until the virus reaches the 5th generation, no effects are visible, but in generation 5 or later there is a 50% chance that the message will appear. In a variant of the virus the message is different:

En tu PC hay un virus RV1,
y sta es su quinta generacin.

It has been reported that this virus was also published in a Greek magazine named "Pixel" in the form of a BASIC program that would create an infected program when run. This program contained a different message:

"Program sick error: Call
doctor or buy PIXEL for cure
description"

A disinfection program, written by the virus author was then published in the next issue of Pixel.

Five other variants of this virus are now known, all from Bulgaria. The major difference is in the length - 852, 740, 345, 299 and 277 bytes. The 740 byte variant is also known as 'Cancer'. It seems that some

virus writers there are competing with each other to create the shortest possible version of the virus. The shortest variant, with a length of 277 displays a different message, "PARITY ERROR", simulating a hardware failure.

- **AntiPascal** — Two viruses, probably from Bulgaria, 605 and 529 bytes long, designed to corrupt .PAS and .BAK files. They are said to have been written as a revenge against a former employer of the virus author. The viruses are added to the front of infected programs.
- **AntiPascal-2** — A group of three viruses, 400, 440 and 480 bytes long, which are similar to the Anti-Pascal viruses, but somewhat different structurally - for example they add the virus code to the end of the programs they infect, rather than the beginning.
- **April 1** — Here we actually have not one virus, but two different viruses, probably written by the same author, somewhere in Israel. One of them infects .EXE files, the other .COM files. The two viruses have the same effect, however. On April 1st an infected computer will display the following message:

APRIL 1ST HA HA HA
YOU HAVE A VIRUS.

The .COM virus is 897 bytes long, but the .EXE virus is a bit longer, 1488 bytes.

Those two viruses were later combined into one, called SURIV 3, which evolved into the Jerusalem virus.

- **Armagedon** — This virus originated in Greece. It is 1079 byte long, infects .COM files, other than COMMAND.COM, by adding itself in front of the original program. This virus has an interesting effect if a Hayes compatible modem is installed in the computer, including dialing the number 081-141. This is the number of the "speaking clock" on the island of Crete.
- **Attention** — This 394 byte Russian virus gets its name from the string

"ATTENTION" which is written near the beginning of infected files. Like most of the other recent Eastern Europe viruses it has not been analyzed yet.

- **Bebe** — This Russian virus contains the following pieces of text:

VIRUS! Skagi "bebe" Fig
Tebe!

A translation is not yet available. This is a 1004 byte virus, which only infects .COM files.

- **Best Wishes** — A 1024 byte .COM infecting virus, containing the text

This programm ... With Best
Wishes!

The virus has not been analyzed yet, but many programs, including COMMAND.COM, will not work properly when infected.

- **Black Monday** — The name of this virus is derived from a text string found inside it:

Black Monday 2/3/90 KV
KL MAL

This is a 1055 byte virus, which will infect .EXE and .COM files. It is not possible to restore infected .EXE files, as the virus may overwrite some bytes at the end of the file.

- **Blood** — A very simple 418 byte non-resident virus from Natal in South-Africa. It was written by a student, who claims to have no knowledge of how it "escaped". This virus, just like Kennedy, will only infect .COM files starting with a JMP statement (E9). Infected programs may occasionally display the following message when they are executed.

File infected by BLOOD
VIRUS version 1.20

Reports of a Blood-2 virus are based on a misunderstanding.

- **Bulgarian Tiny** — This family of viruses currently contains the smallest viruses known - 198, 167, 160, 159, 158, 156, 154, 143, 138, 134 and 133 bytes long. They do nothing of particular interest, but appear to be written in an attempt to write the smallest virus possible.

- **Burger** — This virus was written by R. Burger, author of the Virtem virus. The virus is not a serious threat - a 560 byte destructive/over-writing virus, which is easily noticed as infected programs will not run normally. As with the 405 virus, disinfection is not possible. A few variants, slightly modified, possibly in order to bypass some scanning program are also known.
- **Carioca** — This is a 951 byte .COM virus, which has not been analyzed yet.
- **Cascade** — The Cascade virus, also known as 1701 or 1704, is probably one of the most common viruses around. The problem is just that it is often not detected, because it produces no obvious effects. In the original version, the virus contained code that was set to "go off" between Oct 1. and Dec 31, 1988, shortly after an infected program is run. The effect is actually quite amusing - the characters on the screen fall down and end in a heap on the bottom.

There is a bug in some versions of the virus - it seems that the author intended the virus to infect all computers, except those from IBM. However, it did not work as planned - the virus would also infect "true" IBM machines.

There is one variant of this virus, reported as 17Y4, which is almost identical to the most common 1704 variant. One byte has been changed, probably due to a random "mutation". This, however, has resulted in a "bug" in the virus. Another mutated variant is also known - it infects the same file over and over.
- **Christmas in Japan** — This is a 600 byte virus from Japan, reported to activate on Dec. 25. It only infects .COM files, but has not been fully analyzed yet.
- **DataCrime** — The DataCrime virus was probably written in W. Germany or the Netherlands. It caused much panic around Oct. 13th 1989 when it was set to go off.

Any infected program run on Oct. 13 or later in the year would format the first nine tracks of the hard disk and display the message

DATACRIME VIRUS
RELEASED: 1 MARCH
1989

Since this virus is currently very rare, it is not a serious threat, but it could become a problem in the future.

The two variants of this virus, 1280 and 1168 are practically equivalent, but another virus, called "Data-Crime II" exists as well. It infects .EXE and .COM files, but the original "DataCrime" could only infect .COM files. DataCrime 2 is also a bit larger, 1514 bytes long and more complicated than the original virus. The latest variant, called DataCrime II-B is very similar to DataCrime II, but is only 1480 bytes long.

- **Datalock** — A new, 920 byte virus, which has not been fully analyzed yet. It will infect .EXE files, but only some .COM files including COMMAND.COM.
- **dBase** — The dBase virus is very rare, but rather curious. It is clearly intended to garble dBase files, or rather any file with a name that ends in .DBF.

If the virus is active in memory when a program writes to a .DBF file, it will garble all the outgoing data. However, when the data is read back later, the virus will correct the garbled data.

There is just one problem. If the virus is detected and removed, the data will be useless because the virus will not be present to "de-garble" it when it is read back.

There is a more harmful side to this virus. If an attempt is made to write to a .DBF file that is more than three months old, the virus will try to destroy the FAT and root directory on drives D:, E: ... Z: There is a bug in the code, however, so the destruction will be rather unpredictable.

The dBase virus will only infect .COM files, increasing their size by 1864 bytes.

- **December 24th** — This virus was discovered in Iceland on Dec. 24th 1989. Several computers refused to run any programs at all on that date, but simply displayed the message "Gledileg jol" ("Merry Christmas") instead. The virus is a variant of the Icelandic-2 virus, but with several minor corrections and modifications.
- **Destructor** — The name of this virus is derived from the following string which is stored inside it:

DESTRUCTOR V4.00 (c)
1990 by ATA

This is a 1150 byte virus, which infects .COM as well as .EXE files.

- **Devil's Dance** — A .COM infector reported to have originated in Spain or Mexico. It adds 951 bytes to the end of any file it infects. It will infect the same file over and over until it become too large to fit in memory. The virus traps INT 9 (the keyboard interrupt) and when CTRL-ALT-DEL is pressed it will display the message:

DID YOU EVER DANCE
WITH THE DEVIL IN THE
WEAK MOONLIGHT ?
PRAY FOR YOUR DISKS!!
The Joker

The virus also monitors any keystrokes, activating when 2000 are reached. It will then change the colors of any text displayed on the screen. When 5000 keystrokes are reached the virus will trash the first copy of the FAT.

- **Diamond** — This is a 1024 byte virus from Bulgaria, which has been reported as bearing some resemblance to the "Eddie" virus, possibly written by the "Dark Avenger" as well. The virus makes some effort to disable any debugger

program used to monitor it, but does not seem to do anything of particular interest.

- **DIR** — This Bulgarian virus will infect files when the DIR command is given, hence the name. It is 691 bytes long, and will only infect .COM files, no destructive code has been found in the virus.
- **Doteater** — A rather primitive 944 byte virus, probably written in Poland. It infects only .COM files, and when it activates it will remove all dots (.) from the screen.
- **Durban (Saturday the 14th)** — This virus infects both .EXE and .COM files. It first adds 1-16 bytes to the files it infects length, so they end on a paragraph boundary. Then 669 additional bytes, containing the virus itself are written to the end.
Durban is a resident virus, using a method similar to that used by Jerusalem to check if it already installed.
On any Saturday the 14th, the first 100 logical sectors of drive C, then B, then A are overwritten with rubbish.
- **Dyslexia** — Another name for this virus is "Solano", indicating its origin in Solano county in California. It is 2000 bytes long, adding 1991 bytes in front of .COM files, and 9 bytes at the end. The virus may prevent the proper execution of some programs, but does no serious damage. It is reported to transpose adjacent characters on the screen. The name is hidden in encrypted form inside the virus.
- **Eddie** — This virus contains two interesting text strings:
"Eddie lives...somewhere in time"
and
"This program was written in the city of Sofia (C) 1988-89 Dark Avenger"
"Eddie" is probably the skeleton mascot of the heavy metal band "Iron Maiden". This was the first

virus reported to have originated in Bulgaria, but it was soon followed by many others.

There is only one thing unusual about this virus. It remains resident, just as many other viruses, but it will not only infect a program when it is run, but also when the program file is read. This means that a harmless program that opened each .EXE and .COM file in turn, for example to check them for infection, could easily cause an "epidemic".

The virus will infect .EXE and .COM files, adding 1800 bytes to the length. COMMAND.COM will be one of the first programs to become infected.

When an infected program is run, there is a 1-in-16 chance that the virus will trash a random disk sector.

One 2000 byte variant is known. It is also from Bulgaria, probably written by the same author as the original one. It has been improved a bit - you won't see an increase in file length when you issue a DIR command. The third known variant, also by "Dark Avenger" is 2100 bytes long.

Inside the virus one finds the following string

Copy me - I want to travel
or, in some versions
only the Good die young...

The virus author also included the following string in the virus:

copyright (C) 1989 by
Vesselin Bontchev

Vesselin Bontchev, however, is a Bulgarian author of anti-virus programs, and has nothing to do with the creation of the virus. The reason this message appears is that the virus searches for it in every program executed, and halts the computer when it is found.

The author of the virus - Dark Avenger - has distributed the source and several new viruses can be expected in this family. One has appeared in the Soviet Union. It is

known as "Hymn" and is 1865 bytes long.

- **Eddie II** — A fairly harmless virus from Bulgaria - called "Eddie II" because it contains the string "Eddie lives". This string is similar to the string contained in the original "Eddie" virus. Eddie II can infect .EXE files as well as .COM files, but unlike most other .EXE infecting viruses, it does not pad them so their length becomes a multiple of 16 bytes, before they are infected. Infected files are marked with a value of 62 in the "seconds" field of the timestamp, which makes them immune to infection by Vienna or Zero Bug. Infected files grow by 651 bytes, but this increase will not be seen if a "DIR" command is given, because the virus intercepts the "find-first" and "find-next" functions, and if the "seconds" field contains 62, the virus will decrement the file length by 651. Apart from this the virus does nothing of interest.
- **Fellowship** — The name of this virus is derived from the following text, which can be found inside it:

This message is dedicated to
all fellow PC users on Earth
Towards A Better Tomorrow
And A Better Place To Live
In

The virus is actually not very friendly - it attaches it to the end of .EXE files, but may overwrite the last 20 bytes or so of the original file. The virus itself is 1019 bytes long. It may cause further damage, but it has not yet been analyzed.

- **Flash** — This virus probably originated in Germany. It adds 688 bytes to any .COM or .EXE file it infects. The virus is still awaiting full analysis.
- **Flip** — The Flip virus is 2343 bytes long, and infects both .EXE and .COM files as well as boot sectors of hard disks. When the virus activates on a computer with an EGA or VGA display adapter, it will "flip" the screen horizontally and

switch to a special character set, which reverses each character. This effect only happens on the second day of each month, between 16:00 and 16:59. The method used to infect boot sector is similar to that used by the V-1 virus, except the Flip virus will only infect hard disks, not diskettes.

- **Frodo (4096, IDF)** — The Frodo virus infects both .EXE and .COM files. It is very advanced in some ways, being able to hide the infection by using a method similar to that used by the "Zero Bug" virus. If the virus is active in memory and you look at the directory, the virus will show you the original length of any infected program. The virus seems to be able to cause damage to data, as files may become crosslinked when it is active

It activates on Sept. 22, when it may attempt to place a Trojan on boot sectors. This Trojan will display the message "FRODO LIVES" in large letters on the screen, surrounded by a moving pattern. The code to write the Trojan to the disk seems to be garbled in all known versions of the virus and will probably "hang" the computer.

The length of infected files increases by 4096 bytes, but a variant "Fish 6", 3584 bytes long was recently reported. The effects of this variants are not known yet.

- **Fu Manchu** — The author of the Fu Manchu virus seems to have intended to write one of the most humorous viruses around. He started with the Jerusalem virus, removed the harmful part of it and added several new features:

The virus will censor the text the user types, deleting two four letter words.

It will also take action if the user types "Thatcher", "Reagan", "Botha", or "Waldheim". In those cases it will add comments to the text.

When Ctrl-Alt-Del is pressed, the virus will display the message:

The world will hear from me again!

In other respects the virus is similar to the Jerusalem virus. It will infect both .EXE and .COM files, making them grow by about 2086 bytes.

- **Fumble** — The "Fumble" virus is a small, memory resident .COM infecting virus that will generate typing errors, every now and then. That is, if you press the "R" key for example, it will occasionally insert another letter like "E" in the text instead. The only unusual feature of this virus is that it will only infect programs on odd-numbered days.

Infected .COM files grow by 867 bytes.

- **GhostBalls** — This virus was written in Iceland and first discovered there in October 1989. It contains the following text strings:

GhostBalls, Product of
Iceland Copyright (c) 1989,
4418 and 5F19

It will infect .COM files, making them grow in size by 2351 bytes. Basically it is just the Vienna virus - the variant in the book by Ralf Burger to be specific, with an extra twist. When an infected program is run, the virus will search for other programs to infect, but also try to place a modified copy of the Ping-Pong virus on the diskette in drive A, provided it is a 360K diskette. This Ping-Pong variant has been changed, so that it is not infectious, but it will also work on a '286 machine. This modified boot sector is not a virus, but F-DISINF will remove it.

- **Guppy** — This is simple, 152 byte virus, which only infects .COM files, and may infect the same file over and over. Like the Kennedy virus, it will only infect files starting with a JMP.
- **Hallchen** — This is a .COM and .EXE infector, probably written in W-Germany. It contains two text strings:

Hallchen !!!!!, Here I'm..
Activate Level 1..

This virus is a bit unusual in some ways - for example it will not infect "old" files. If the value of the "month" or "year" fields in the timestamp is different from the current date, the file will not be infected.

The virus does not modify the creation date when it infects the virus, and like most other viruses it is easily able to defeat the read-only attribute. It will only infect files larger than 5000 bytes, increasing their length by 2011 bytes.

The major effect is reported to be garbling of keyboard input.

- **Icelandic** — This virus was first found in Iceland in June '89. If only infects files with names ending in .EXE. When an infected program is run, it will hide in memory by directly manipulating the Memory Control Blocks. Programs that watch out for any program "going TSR" will therefore not be able to catch it.

This virus will mark one cluster on the hard disk as bad, every time it infects a file.

A minor variant of this virus was later found in Saratoga, and a radically modified version appeared in Iceland in July '89. This new version (Icelandic-2) does not use INT 21 calls like the original, but instead makes direct JMPs into the operating systems. This means that many protection programs will be unable to catch it. Icelandic-1 is 656 bytes long, Saratoga is 642 bytes but Icelandic-2 adds 632 bytes to any file it infects. Actually the file may grow a bit more because all the viruses will first pad the file so the length becomes a multiple of 16 bytes.

- **Internal** — A 1381 byte .EXE-infecting virus, which may occasionally garble the screen and display a fake error message.
- **Itavir** — This is a fairly long, 3880 byte, Italian .EXE file infector. The virus is reported to activate after the

system has been left running for at least 24 hours. It will then corrupt the boot sector, write out a message in Italian, and start writing random values to all I/O ports. This is reported to cause a "hissing" sound from some VGA monitors.

- **Jerusalem (Israeli "Friday 13.")** — The Jerusalem virus is one of the oldest and most common viruses around. As a result there are numerous variants of it. It will infect both .EXE and .COM files, but the first version of the virus contained a bug, causing it to infect .EXE files over and over, until they became too large for the computer. Needless to say, this has been fixed in later releases, including one called "New Jerusalem". Infected files grow by 1808 bytes or so.

The original Jerusalem virus would activate on every Friday the 13th, deleting programs run on that day. 30 minutes after an infected program is run, the virus will also cause a general slowdown of the computer and make a part of the screen scroll up two lines. This has been disabled in some variants of the virus, which makes them much harder to detect.

The first variant of the virus (SURIV 3.00) produced the side-effects described above 30 seconds after an infected program was run.

One variant, "Century" will become active on Jan 1, 2000. It will try to delete everything that can be deleted and then display the message:

Welcome to the 21st Century

The programmer does not seem to have known that the 21st century does not start until a year later.

The "Sunday" virus is another variant of the Jerusalem virus. Instead of activating on Friday the 13th, it will activate if the current day of the week is Sunday and display the message:

Today is SunDay! Why do you work so hard?

All work and no play make you a dull boy!
Come on! Let's go out and have some fun!

Apart from this the viruses are very similar. A second variant, Sunday-2 is also known, containing some minor changes.

Other variants include Payday, Anarkia, PSQR, Mendoza, Puerto, Spanish, Westwood and A-204, which are only different in minor ways - different activation dates and other minor changes. Sometimes the changes only involve the reordering of a few instructions, perhaps to prevent the virus from being detected by some virus scanning program. Perhaps the most unusual variant is "Frere", which is reported to play "Frere Jacques" on Fridays, when it activates and "Groen Links", a Dutch variant, which plays a tune whose name translates to "Vote Green Left" ("Green Left" is a political party there).

- **Jo-Jo** — This virus is a 1701 byte, memory resident .COM infector, which is basically a patched, non-encrypted variant of the Cascade virus. It is reported to have originated in Barcelona or Israel. It contains a check for the IBM copyright message at address F000:E008, just like Cascade. The virus contains two text strings:

Welcome to the JOJO virus.
F—k the system (c) - 1990

- **Joker** — This virus is probably extinct, but it originated in Poland, and is 11000 bytes long. It will overwrite .EXE files, and is therefore easily detected. Infected programs will display silly messages when executed, like Water detect in Co-processor I'm hungry Insert HAMBURGER in drive A:
- **Joker-01** — This is also a large Polish virus - 29233 bytes long. It infects files in the same way as Vaccina - .COM files are infected normally, but .EXE files are converted to files with .COM structure, by ad-

ding a small, 139 byte loader program to them.

- **July 13th** — This virus is designed to activate on July 13th - which happened to fall on a Friday in 1990. It is a 1201 byte encrypted .EXE file infector, which has not been fully dissected yet.
- **Kemerovo** — A primitive, 257 byte direct-action Russian virus, which only infects COM files. It has not been fully analysed yet.
- **Kennedy** — A simple .COM infecting virus, probably from Denmark. When an infected file is run, it will infect a single .COM file in the current directory, adding 333 bytes to the end of the file. The virus activates on three dates - June 6th, November 18th and November 22nd. On those dates it will display the message:

Kennedy er dd - Inge leve
"The Dead Kennedys"

There have been reports that infection by this virus may cause FAT corruption, crosslinking of files and loss of clusters, but I have not been able to verify this.

Another variant is also known - which is one of the shortest virus known - only 163 bytes long. This variant seems to do nothing but replicate. Like the original Kennedy virus, this variant, which is known as 'Tiny' has only been reported in Denmark. It is somewhat carelessly written - it does not close the files it opens, for example.

- **Lehigh** — The Lehigh virus is rather unusual in that it only infects one program, COMMAND.COM. It does not increase the size of the program, because it overwrites the stack space. This virus is rather badly written - it can be defeated by simply making COMMAND.COM read-only. It is, however, very destructive. "Lehigh" contains an infection counter and when it has reached a specific number of infections it will trash the disk. This means that the virus never got a

chance to spread much outside Lehigh University.

- **Leprosy-B** — The name of the virus is derived from the following message found inside it.

ATTENTION! Your computer has been afflicted with the incurable decay that is the fate wrought by Leprosy Strain B, a virus employing Cybernetic Mutation Technology(tm) and invented by PCM2 08/90.

Infected programs will either display this message or

Program too big to fit in memory

This is a 666 byte overwriting virus, and disinfected programs must be deleted, as there is no way to remove the virus.

- **Liberty** — Liberty originated in Indonesia. It is a resident .EXE and .COM infecting file, 2857 byte long. The virus code is placed at the end of the file, but the virus also overwrites the first 120 bytes with code and the following message:

- M Y S T I C -
COPYRIGHT (C)
1989-2000, by
SsAsMsUsEsL

A second variant, 2867 byte long is also known. The effects of the viruses are not fully known yet.

- **Loziasky** — This is a Russian, 1023 byte virus, which uses a simple encryption method. It only infects COM files, but has not been fully analyzed yet.
- **MG** — MG stands for "Matematicheskya Gimnazia", the name of the school in Varna in Bulgaria where the virus seems to have been written. This is a 500 byte .COM virus, which hides itself in the upper half of the interrupt table, causing programs like Netware to crash.
- **MG-3** — A 500 byte virus, which only infects .COM files. Awaiting analysis, but is probably related to the MG virus.

- **MGTU** — A very simple, 273 byte Russian virus. It does not remain resident in memory, but will infect COM files when infected programs are run.

- **MIX1** — MIX1 was probably written in Israel, but it is derived from the Icelandic virus. There are two versions known, MIX1 and MIX1-B, practically identical. MIX1 displays a bouncing ball on the screen, and garbles all output going to the printer. It will also disable the NumLock key. MIX1 is larger than the Icelandic virus - 1618 or 1636 bytes, depending on the version.

One unusual "feature" of MIX1 is that it will only infect files 8192 bytes long or larger.

- **MLTI** — This 830 byte Russian virus contains the text:

Eddie die somewhere in time! This program was written in the city of Prostokwashino (C) 1990 RED DIAVOLYATA Hello! MLTI!

The text is more understandable if one considers the similar text found in the "Eddie" virus written by Dark Avenger.

- **Murphy** — The authors of this virus are known. They are Lubomir Mateev Mateev and Iani Lubomirov Brankov, both in Bulgaria. Murphy is a 1277 byte long, resident .COM and .EXE infecting virus. It is based on the Dark Avenger, but is not harmful. Inside it the following message can be found.

Hello, I'm Murphy. Nice to meet you friend. I'm written since Nov/Dec. Copywrite (c)1989 by Lubo & Ian, Sofia, USM Laboratory.

Another variant is also known. It is a bit longer, 1521 bytes, and the message is different:

It's me - Murphy. Copywrite (c)1990 by Lubo & Ian, Sofia, USM Laboratory.

Originally this virus was reported to jump into ROM basic every exact

hour, possibly causing some clones to "hang", but the variant available to researchers in the West produces the "Bouncing Ball" effect every time INT 18 is executed.

- **Nina** — This virus is only 256 bytes long, and derives its name from a the text string found at the end, which says simply "Nina". Like many other small viruses, this one is written in Bulgarian.
- **Nomenklatura** — This virus appears to be of Bulgarian origin, as it contains a message in Bulgarian. This is a 1024 byte virus, which corrupts data on the disk, by modifying the FAT.
- **Number of the Beast** — Like quite a few other viruses, this one was first reported in Bulgaria. It is 512 bytes long, but the length of infected files does not appear to increase. This is because the virus overwrites the first 512 bytes of the programs it infects with itself, and stores the original 512 bytes in the unused space after the end of the file. This is possible because DOS allocates file space in "clusters", which are usually 1024 or 2048 bytes long.

In addition, if a program attempts to read from an infected file, while the virus is active in memory, the read operation will be intercepted and instead of finding the virus, the original code will be read instead.

This means that the virus will be able to fool any checksum program, as well as any virus-scanning program if it is active in memory when the program is run. It does not matter how sophisticated the checksum algorithm is - if the virus is active in memory, no infected program can be detected. F-DRIVER will, however, stop the virus.

At the end of the virus code, the string "666" appears - hence the name. Several new variants are also known in Bulgaria, where this string is missing, but they are functionally identical. ■

The Best of the BBS

Edited by Mark Thacker, VAX Programmer/Operator (Mark@UNT.VAX)



Welcome to the **Best of the BBS** column. This column highlights some of the more interesting and useful discussions on the UNT BBS. For those of you not familiar with the BBS, here is how to log into the UNT BBS.

- Sign-on by typing **CALL DEC** at the LAN prompt and then entering **BBS** as your Username at the **VAX** prompt.
- If you are already logged-on to the VAXcluster, type **BBS** at the \$ prompt.

*The opinions expressed in this column do not necessarily reflect the views of Academic Computing Services or the Computing Center. Also, information in **Best of the BBS** has not been checked for accuracy.*

Coherent

#1552 2-FEB-1991 23:13:12.94

Subject : COHERENT

Does anybody out there besides me have Coherent, the \$99 UNIX clone? I would be interested in hearing from anybody who has written code for both Coherent and various other flavors of UNIX who could say something about similarities/differences.

#1562 Reply to #1552 4-FEB-1991 14:06:02.04

Subject : RE: COHERENT

Hi David, When I first saw the add for Coherent I called and talked to the developers to find out what it was and what it wasn't. I won't waste the bandwidth repeating every word he said. According to what I heard, all of programs and data for all of the process' must fit into one 64K segment.

This is not as bad as it sounds since the C programs compile to very small size under Coherent. I hear that it's quite nice to use as a UUCP node but there is no support for ethernet or X-windows. I figure that it is probably not a bad thing to get to begin to learn your way around UNIX but it probably isn't so hot to get real work done. For \$99 dollars you wouldn't be out much even if it did suck. btw, there is an article about Coherent in the latest issue of UNIX World. ■

Disk Backup Schedules

SYSTEM	BACKUP	DESCRIPTION
Administrative MVS/SP	Daily	Monday - Friday around 7 p.m. (after COM-LETE is shut down) & on Saturday & Sunday if COM-LETE has been up that day.
	Weekly	Full pack dumps taken each Sunday morning.
	Monthly	Full pack dumps taken on the first day of each month.
Academic MVS/SP	Daily	Monday - Sunday during the early hours of the morning.
	Weekly	Full pack dumps taken each Sunday.
	Monthly	Full volume dumps taken on the first day of each month.
MUSIC/SP	Daily	Wednesday - Monday starting at 4 a.m. and lasting about 30 minutes.
	Weekly	Tuesday mornings at 3 a.m., these last about 2 hours.
	Semester	Once a semester, a permanent backup is taken.
VM/XA	VM Weekly	Early every Wednesday morning.
	CMS mini-disks	Daily backup performed early every morning. Weekly backup every Tuesday starting after Midnight.

Get a Subscription to *Benchmarks*

Benchmarks is a vital link between the UNT Computing Center and the users of our facilities. It is important for all users of the computing facilities to maintain a file of these newsletters because they contain materials which will periodically update existing documents as well as information and suggestions on uses of OS/MVS, MUSIC/SP, the VAXcluster, Microcomputers, and other resources available to UNT students and faculty. To facilitate the dispersal of *Benchmarks*, *** FREE *** subscriptions are available. To receive yours, send the following information to us either by snail mail (the post office or campus mail), FAX (817) 565-4060, or through electronic mail, to the UserID AS04 on MUSIC, VMS, or CMS.

Name: _____

Mailing Address: _____

PLEASE GIVE A CAMPUS ADDRESS (NOT BOX) IF POSSIBLE! - It's Cheaper !!

___ Renewal ___ Change of Address ___ Cancel Subscription

Academic Computing Services
The Computing Center
NT Box 13495
University of North Texas
Denton, TX 76203
FAX 817-565-4060

